

Dell Wyse Configuration
(WCM) Manager
Release 1.3.0.0

Administrator's Guide



Notes



NOTE: A NOTE indicates important information that helps you make better use of your computer.

© 2013 Dell Inc. All rights reserved.

Trademarks used in this text: Dell™, the Dell logo, vWorkspace®, and Wyse® are trademarks of Dell Inc. Microsoft®, Windows® Embedded Standard 2009, Windows® Embedded Standard 7, Windows® Embedded Standard 8, Windows Server®, and Internet Explorer®, are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. .

Contents

- 1 Introduction 7
 - Overview 7
 - Key Features 8
 - What's New 9
 - Supported Dell Wyse Thin Client Systems 11
 - Supported Operating Systems 13
 - Dell Wyse Technical Support 13
 - Related Documentation and Services 13
 - Dell Wyse Online Community 14
- 2 Installing and Configuring Dell Wyse Configuration Manager (WCM) 15
 - Pre-requisites to Install WCM. 15
 - Downloading and Installing WCM 17
 - Downloading WCM. 17
 - Installing WCM Server Application 17
 - Installing WCM Client 18
 - The WCM Environment 18
 - Configuring the Repository Server 19
 - Configuring the Repository Server on a Windows 2003/Windows 2003 R2 Server. 19

	Configuring the Repository Server on a Windows 2008/Windows 2008 R2 Server	22
	Configuring the Repository Server on a Windows 7 System	24
	Discovery Settings for the WCM Server.	26
	DNS Service Record Lookup	26
	DNS Hostname Lookup	30
	DHCP Option Tags Lookup	32
	Configuring the WCM Thin Client Systems	36
	Configuring the Dell Wyse Device Manager (WDM) Server	37
3	Using the Dell Wyse Configuration Manager (WCM) GUI Application	39
	About the WCM Application GUI	39
	Creating New Configuration Files	41
	Editing Existing Configuration Files	42
	Configuration Details	42
	Connections.	43
	Device Configuration	53
	OS Configuration	63
	Agent Settings	69
	Using Your Configuration Files	70
	Setting Up Automatic Configuration	70
	Setting Up Manual Configuration.	71

4	Using the Dell Wyse Configuration Manager (WCM) Client	73
	Launching the WCM Client	73
	Importing Thin Client Configurations	73
	Fallback Mechanism for Failed Download of Configuration File.	74
	Exporting Thin Client Configurations	75
	Using Configuration History	75
	Manually Setting Debug Options on a Thin Client	76
5	Typical Use Case Scenarios	77
	Case 1 - Using a Single Configuration for Multiple Thin Client Users.	77
	Case 2 - Using Multiple Configuration Files for Multiple Thin Client Users.	78
	Case 3 - Editing Specific Configuration Files for Thin Client Users.	78
	Case 4 - Selecting Specific Configuration Files Using a Thin Client on the Network	79
	Case 5 - Applying Specific Configuration Files to a Mobile Thin Client	79
	Case 6 - Applying Configuration Files for New or Different Thin Client Users	80

A	Appendix	81
	Troubleshooting Devices That Cannot Locate Configuration Files.	81

Introduction

Dell Wyse Configuration Manager (WCM) is an innovative self-configuring client technology for the cloud and Dell Wyse Enhanced Embedded virtual desktop environments. WCM provides a simple solution to create and apply configuration files to Dell Wyse thin clients running supported Microsoft Windows Embedded operating systems.

WCM is mainly used by IT Administrators who create configuration files using a simple standalone GUI or capture them from an already configured Dell Wyse thin client running a supported Windows Embedded operating system. The thin client system connects to the remote file folder location that contains the configuration file and downloads the same to update the configuration. WCM enables configuration of multitude of thin clients without a management server.

This guide is intended for administrators of Wyse thin clients running WES2009, WES7, WES7p, or WE8S. It provides the necessary information for using the tool to create and apply configuration files to Wyse thin clients.

The supported Windows Embedded operating systems are:

- Wyse Embedded Standard 2009 (WES2009)
- Wyse Enhanced Microsoft Windows Embedded Standard 7 (WES7)
- Wyse Enhanced Microsoft Windows Embedded Standard 7 p (WES7p)
- Wyse Enhanced Microsoft Windows Embedded 8 Standard(WE8S) (32-bit and 64-bit)

Overview

WCM helps you to easily deploy thin client configurations either manually or through a server environment and is an easy-to-use solution for supported Windows Embedded thin clients from Dell Wyse.

WCM consists of two components:

- **WCM Application GUI** — is a standalone GUI to create new configuration files as well as edit existing configuration files. These files can be placed on an FTP server (for FTP) or on a Web server (Microsoft IIS Web server for HTTP or HTTPS) in order to be deployed on thin clients running the WCM Client.
- **WCM Client** — is a client component that is pre-installed or deployed in the supported thin client systems by using the Dell Wyse Device Manager (WDM). After you log in to the thin client system, the **WCM Client** downloads the latest configuration file and applies the configurations. As an administrator, you can also use the WCM Client Control Panel applet to export the current customized configurations of a thin client as a configuration file, and to manually import configuration files into the thin client.

You can deploy the WCM configuration files to your thin clients both automatically and manually. For more information, see [Setting Up Automatic Configuration](#), [Setting Up Manual Configuration](#), and [Importing Thin Client Configurations](#).

The following diagram describes the deployment of configuration files on a WCM thin client.



Key Features

The WCM has the following features:

- Provides granular control to deploy:
 - Universal, or user-specific settings
 - Stationary or mobile thin clients
 - Local or remote devices

- Provides the ability to:
 - Create configuration files from a standalone GUI or capture the configuration from an already configured device
 - Maintain history of configurations
 - Update existing configurations or revert to previous configurations
 - Use the **Appliance mode** to configure one or more Windows Embedded thin clients to function as a simple-to-use, dedicated kiosk for one of the following:
 - Citrix Clients
 - VMware View Clients
 - vWorkspace Clients
 - Microsoft RDS/RDP Clients
 - Internet Explorer
 - Use the Generic Appliance mode for any user-specified application.

What's New

The new features in this release of WCM are:

- Support for thin clients running WE8S (32 bit and 64 bit)
- Support for Appliance Mode for any user-specified application (Generic Appliance Mode)
- Support for configuring Quest vWorkspace clients
- Support for creating Internet Explorer URL shortcuts on the desktop for the selected favorites
- Support for configuring an Exit button on the Citrix Enterprise Receiver Appliance Mode in the Published Apps or Desktops dialog box. This button enables you to exit from the Appliance Mode

- Support for **Exit** button for all Appliance Modes applications. This allows the user to exit, log off, shut down or restart from the client while in Appliance Mode. This feature is also supported for other Citrix XenDesktop and VMware Horizon View Appliance Mode applications with some limitations. This release also supports the ability to configure the exit buttons and shortcuts per user.
- Support to configure share drives from the WCM Client. You can add or remove share drive connections and also map the remote machine drive by using Share Drive.
- Single sign-on (SSO) for domain joined devices. This version of WCM provides the single sign on feature for domain joined devices to connect using RDP, VMware View, Citrix Xenapp.
- Support for Adobe Flash Player settings. You can use the WCM 1.3 Client to configure Adobe Flash player for Citrix sessions.
 - **Flash Remoting:** Enables HDX Media Stream Flash Redirection on the user device.
 - **Server Http Cookies:** Enables synchronization of the client-side HTTP cookies with the server-side in order to download HTTP cookies from the server.
 - **Server Side Content Fetching:** By default, the HDX Media Stream Flash Redirection downloads Adobe Flash content to the user device and plays the content.
 - **URL rewriting rules for client-side content fetching:** One can redirect an attempt to obtain Flash content using the URL rewriting rules for client-side content fetching setting which is a second generation Flash Redirection feature.
- Removal of WebDAV dependency for both HTTP and HTTPS protocol to download the configuration files or resource files.
- Ability to block or unblock the popups on a Citrix Session when connecting to a full screen ICA session on the WCM Client.
- Support for RDP 8 settings.

- WCM 1.3 client supports RDP8 and its new features. The settings given below are supported for RDP8 functionality by WCM.
 - Detect Connection Quality automatically
 - Remote Desktop Gateway KDC proxy and Edit box option for KDC Proxy Name
 - Enable Workspace Reconnect
- Ability to configure Citrix Standard Receiver using the WCM Client.
- Enhanced speed of download and applying of configuration on the thin client systems.

Supported Dell Wyse Thin Client Systems

WCM is supported on the following thin client systems that run:

- Wyse Enhanced Microsoft Windows Embedded Standard 2009 build 684, 685, 686, 703, 704, 716, 718, 719, 720, 723, 716, 727 or later:
 - C90LEW
 - D90DW
 - R90LW
 - R90LEW
 - R90LW Fiber-NIC Ready
 - V90LEW
 - X90cw
 - X90mw
 - X90LW
 - X90LeW
 - Z90DW
 - Z90SW

- Wyse Enhanced Microsoft Windows Embedded Standard 7 build 818, 827, 830, 832, 833, 846, 858 or later:
 - C90LE7
 - D90D7
 - D90Q7
 - R90L7
 - R90LE7
 - X90C7
 - X90M7
 - Z90D7
 - Z90DE7
 - Z90S7
 - Z90Q7
- Wyse Enhanced Microsoft Windows Embedded Standard 7p build 850 or later:
 - X90M7p
 - Z90D7p
 - Z90DE7p
- Wyse Enhanced Microsoft Windows Embedded 8 Standard build 904, 907, and 908:
 - D90D8
 - D90D8x
 - D90Q8
 - Z90D8
 - Z90D8x
 - Z90Q8



NOTE: If you have thin clients running earlier builds where the WCM Client was not pre-installed on your thin client, you can:

- Re-image the thin clients with the latest firmware to include the WCM Client in those builds.
- Use WDM to push the WCM Client package to each thin client.
- Install the WCM Client manually. Ensure that you disable the File Based Write Filter on the thin client before installing the WCM Client.

Supported Operating Systems

WCM is supported on Dell Wyse thin clients running the following operating systems:

- WE8S (32-bit and 64-bit)
- WES7P
- WES 7
- WES 2009

Dell Wyse Technical Support

To access Dell Wyse technical resources, visit <http://www.wyse.com/support>. If you still have questions, you can submit your questions using the Dell Wyse Self-Service Center at <http://support.wyse.com/selfservice.html> or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

To access international support, visit <http://www.wyse.com/global>.

Related Documentation and Services

Fact Sheets containing features of hardware products are available on the Dell Wyse Web site. Go to <http://www.wyse.com/products> and use the Cloud clients tab to locate and download the Fact Sheet for your hardware product.

If you need to upgrade your Windows Embedded Standard operating system, contact Dell Wyse Customer Support at: <http://www.wyse.com/support>.

Dell Wyse Online Community

Wyse maintains an online community where users of our products can seek and exchange information on user forums. Visit the Wyse Online Community forums at: <http://community.wyse.com/forum>.

Installing and Configuring Dell Wyse Configuration Manager (WCM)

This section provides information about installing and configuring WCM in your environment. Depending on your environment and intended deployment, you can choose one of the following:

- **Server Deployment** — if you want a server environment that uses FTP, HTTP, or HTTPS servers and intend to create configuration files that thin clients can access automatically to update themselves.
- **Manual Deployment** — if you want a non-server environment and intend to create configuration files that thin client systems can access locally to update themselves manually using the Import feature of the WCM Client Control Panel applet on the thin client system.

Pre-requisites to Install WCM

The pre-requisites mentioned in this section are applicable to both manual and server deployment modes.

To install WCM on a server, ensure that the server meets the following requirements:

- 1 Ensure that the following hardware requirements are met on the server:
 - **CPU** — A minimum of 1 GHz Intel or AMD X86. We recommend a 2.4 GHz Dual Core Intel or AMD X86 CPU.
 - **RAM** — A minimum of 512 MB. We recommend 2GB.
 - **Free Space** — A minimum of 500 MB. We recommend a free space of 720 MB. The actual free space required depends on:
 - The number and size of the configuration files you store
 - The number of thin client devices you manage

2 Install the supported operating system on the server for the WCM Application. The supported operating systems are:

- Windows 7 Professional Enterprise Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2003
- Windows Server 2003 R2

The supported operating system languages to install the WCM Application are:

- Chinese Simplified
- English
- French
- German
- Japanese
- Spanish
- Russian

3 Install Microsoft .NET framework 3.5 or higher on the server.

4 Ensure that Internet Information Services (IIS) version 6.0, 7.0, or 7.5 is installed.

5 Ensure that all required communication ports are available and open for proper communication between servers, routers, and switches. The server port requirements for FTP, HTTP, and HTTPS are:

- FTP – Port 21 with defaults
- HTTP – Port 80 with defaults
- HTTPS – Port 443 with defaults



NOTE: Steps 4 and 5 are not required for Manual Deployment.

Downloading and Installing WCM

Downloading WCM

The WCM software package includes:

- The installer for WCM Server Application
- The installer for locally installing the WCM Client on an individual thin client.
- Packages for remotely deploying the WCM Client onto multiple thin clients using Dell Wyse Device Manager (WDM).

To download the WCM software package:

- 1 Launch the internet browser and navigate to the Dell Wyse support site at <http://www.dellwyse.com/serviceandsupport/support/downloads.asp>.
- 2 Select **Wyse Configuration Manager** from the **Product Downloads** → **Active** drop-down box.
- 3 Click **Search**. The downloads for WCM are displayed.
- 4 Click the latest version of the WCM build. The EULA page is displayed.
- 5 Select the **I Agree** option and click **Next**.
- 6 Navigate to the location where you want to save the .zip file that contains the WCM installer.
- 7 After you download the .zip file, extract the contents.

Installing WCM Server Application

To install the WCM server application, run the **Wyse Configuration Manager Application.msi** file and follow the wizard to install the application. The default location for installation is **C:\Program Files\Wyse\WCM\Application**.

Installing WCM Client

The WCM Client is included in supported Windows Embedded thin clients. To update them you can:

- Install them manually on each thin client, as an administrator.
- Deploy them remotely, to multiple thin clients, using the Dell Wyse Device Manager (WDM). Register the WCM Client into WDM and then deploy it to multiple devices remotely. For more information on registering the WCM Client into WDM, see the *WDM Administrator's Guide*.

To install the WCM Client manually:

- 1 Log in to the thin client system as an administrator.
- 2 Disable the file based write filter (FBWF).
- 3 Run the **Wyse Configuration Manager Agent_LaunchPad.exe** file and follow the wizard to install the WCM client.
- 4 Restart the thin client system when prompted.
- 5 When the installation is complete, re-enable the FBWF. The WCM service does not work when the FBWF is disabled as it does not download and apply the XML configuration file.

The WCM Environment

The WCM environment consists of the following components:

- **Repository Server** — This is the server where the WCM configuration files are copied and the WCM GUI is installed.



NOTE: You can install the WCM GUI on a separate server and store the WCM configuration files on a separate server.

- **DNS/DHCP Server** — This is the server where you configure the Domain Name Server (DNS) or the Domain Host Configuration Protocol (DHCP). DNS or DHCP settings are used by the WCM client to find the Repository server with WCM configuration files. For more information, see [Discovery Settings for the WCM Server](#).
- **WCM Client Software on Thin Client Systems** — These are the thin clients with WCM Client software, which download the configuration files from the repository server.

For WCM to work, you need to configure each of the components.

Configuring the Repository Server

Configuring the Repository Server on a Windows 2003/Windows 2003 R2 Server

- 1 Log in to the repository server as Administrator.
- 2 On the Start menu, go to **Control Panel** → **Add or Remove Programs** and click **Add/Remove Windows Components**.
- 3 Select **Application Server** in the **Windows Components Wizard** and click **Details**.
- 4 In the **Application Server** window, select **Internet Information Services (IIS)** and click **Details**.
- 5 In the **Internet Information Services (IIS)** window, select **File Transfer Protocol (FTP) Service**, **Internet Information Services Manager**, and **WorldWide Web Service**.
- 6 Click **OK** to go back to the **Application Server** window, and **OK** again to go back to the **Windows Components Wizard**.
- 7 Click **Next** to install IIS.
- 8 Navigate to **C:\inetpub\ftproot** directory and create the following directory structure under them:
 - Wyse
 - WE8S
 - WES
 - WES7

- 9 Launch IIS Manager, select **Default Web Site**, right click and select **New** → **Virtual Directory** on the menu.
 - a In the **Virtual Directory Creation Wizard**, enter **WCM** under **Alias** and click **Next**.
 - b Navigate to the physical location of the Wyse folder structure that you created in step 8. For example, **C:\inetpub\ftproot**.
 - c Click **Next**.
 - d Enter the type of access to the folder such as **Read**, **Write**, **Browse** etc.
 - e Click **Next** to complete the wizard. The virtual directory is created with the Wyse folder structure.
- 10 Verify the FTP virtual directory structure under **FTP Sites** → **Default FTP Site**. It is automatically created.
 - a Right-click **Default FTP Site** and select **Properties** on the menu.
 - b In the **Default FTP Site Properties** window, click the **Home Directory** tab to verify the virtual directory.
- 11 Set up the ports for FTP, HTTP, and HTTPS.

Setting up the FTP port on a Windows 2003 Server

- 1 Launch IIS Manager, right click **Default FTP**
- 2 Select **New** → **FTP Site** on the menu. In the **FTP Site Creation Wizard** click **Next**.
- 3 Type **WCM** in **Description**, and click **Next**.
- 4 The default **Port** number is displayed as **21**. Leave the default port number.
- 5 Under **Enter the IP address to use for this FTP site** leave the default value and click **Next**.
- 6 Leave the default settings for **FTP User Isolation** and click **Next**.
- 7 Browse to the FTP Directory (**C:\inetpub\ftproot**) and click **Next**.
- 8 Enter access to the FTP Directory and click **Next** to complete the setup.

Setting up the HTTP and HTTPS Ports on a Windows 2003 Server

- 1 Launch IIS Manager, select **Default Web Site** and right click.
- 2 Select **New** → **Web Site** on the menu. In the **Web Site Creation Wizard** click **Next**.
- 3 Type **WCM** in **Description**, and click **Next**.
- 4 The default **Port** number is displayed as **80**. Leave the default port number. This is the default HTTP port.
- 5 Under **Enter the IP address to use for this FTP site** leave the default value and click **Next**.
- 6 Browse to the website home directory **C:\inetpub\ftproot** and click **Next**.
- 7 Enter access to the website home directory and click **Next** to complete the setup.
- 8 To configure the HTTPS port:
 - a Right-click on the newly created website, and select **Properties** on the menu.
 - b In the **Properties** window, on the **Web Site** tab, enter the **SSL port** as 443.
 - c Click the **Directory Security** tab and click **Edit** in the **Secure Communications** section.
 - d In the **Secure Communication** window, select **Require secure channel (SSL)** and click **OK**.
 - e Click **Server Certificate** to create an SSL certificate, if you have not downloaded a certificate for the server. For more information on creating an SSL certificate, see Microsoft KB article 228991 available at <http://support.microsoft.com/kb/228991>.

Configuring the Repository Server on a Windows 2008/Windows 2008 R2 Server

- 1 Log in to the repository server as administrator.
- 2 Launch the **Server Manager** by navigating to **Start**→ **Administrative Tools** → **Server Manager**.
- 3 Select **Roles** on the left pane and click **Add Roles** on the right pane to launch the **Roles Wizard**.
- 4 Select **Server Roles** on the **Roles Wizard** and select the **Web Server (IIS)** option.
- 5 Click **Install** to install the Web Server (IIS).
- 6 Click **Role Services** on the **Roles** pane in Server Manager to launch the **Role Services Wizard**.
- 7 Select the **FTP** and **HTTP** options and click **Install**.
- 8 Navigate to **C:\inetpub\ftproot** or **C:\inetpub\ftproot** directories and create the following directory structure under them:
 - Wyse
 - WE8S
 - WES
 - WES7
- 9 Launch IIS Manager, right click **Default Web Site** and select **Add Virtual Directory** on the menu.
 - a In the Add Virtual Directory window, enter **WCM** under **Alias**.
 - b Navigate to the physical location of the Wyse folder structure that you created in step 8. For example, **C:\inetpub\ftproot**.
 - c Click OK. The virtual directory is created with the Wyse folder structure.
- 10 Verify the FTP virtual directory structure under **defaultFTP**. The virtual directory is automatically created.
- 11 Set up the ports for FTP, HTTP, and HTTPS.

Setting up the FTP Port on a Windows 2008 Server

- 1 Launch IIS Manager, right click **defaultFTP**.
- 2 Select **Bindings** on the menu options.
- 3 In the **Site Bindings** window, click **Add**. The **Add Site Binding** window is displayed.
 - a Select **FTP** under **Type**.
 - b The default **Port** number is displayed as **21**. Leave the default port number.
 - c Click **OK**.
- 4 Click **Close** to exit from the **Site Bindings** window.

Setting up the HTTP and HTTPS Ports on a Windows 2008 Server

- 1 Launch IIS Manager, right click **Default Web Site**.
- 2 Select **Bindings** on the menu options.
- 3 In the **Site Bindings** window, click **Add**. The **Add Site Binding** window is displayed.
 - a Select **http** under **Type**.
 - b The default **Port** number is displayed as **80**. Leave the default port number.
 - c Click **OK**.
 - d For setting up the HTTPS port, select **https** under **Type**.
 - e The default **Port** number is displayed as **443**. Leave the default port number.
 - f Under **SSL certificate**, select the SSL certificate that you have downloaded for the server. For more information on creating an SSL certificate, see Microsoft KB article 228991 available at <http://support.microsoft.com/kb/228991>.

Configuring the Repository Server on a Windows 7 System

- 1 Log in to the repository server as Administrator.
- 2 Click **Start → Control Panel → Programs and Features**.
- 3 Click **Turn Windows features on or off** to launch the **Windows Features** dialog box.
- 4 Expand the **Internet Information Services (IIS)** option to display the additional categories of the IIS features.
- 5 Select the following options under IIS:
 - FTP Server
 - Web Management Tools
 - World Wide Web
- 6 Ensure that the **WebDAV Publishing** option under **World Wide Web Services → Common HTTP Features** is unchecked.
- 7 Click OK to start the installation. After the installation completes, IIS is installed with a default configuration on Window 7.

Setting up the FTP Port on a Windows 7 System

- 1 Launch the IIS Manager.
- 2 Under **Connections**, right click **Sites** and click **Add FTP Site**.
- 3 In the **FTP Site Window**, enter **FTP** under **FTP site name**, and enter the physical path as **C:\inetpub\ftproot**, and click **Next**.
- 4 Enter **All Unassigned** under IP Address, and **21** under Port.
- 5 Select the option **Start FTP Site Automatically**.
- 6 Select the **No SSL** radio button and click **Next**.
- 7 Select **Anonymous** and **Basic Authentication**.
- 8 Select **Allow access to All Users**.
- 9 Grant the **Read** and **Write** permissions and click **Finish**.

Setting up the HTTP and HTTPS Ports on a Windows 7 System

- 1 Launch the IIS Manager.
- 2 Under Connections, right click **Default Websites** and click on **Add Application**.
- 3 In the **Add Application** window, enter the following details:
 - **Alias Name** – WCM
 - **Physical Path** – C:\Inetpub\wwwroot
- 4 Click **OK** and go to the WCM Directory created under **Default Web Site**.
- 5 Expand Compression under the WCM Directory and uncheck the options **Enable Dynamic Content Compression** and **Enable Static Content Compression**.
- 6 Click **Apply** and confirm the IIS installation by typing **http://localhost** in your browser.
- 7 Navigate back to the **IIS Home Page** and click **Server Certificates**.
- 8 Click **Create Domain Certificate** on the right side of the window to display the **Create Certificate** window.
- 9 Enter significant values for all the fields and click **Next** to display the **Online Certificate Authority** Window.
- 10 On the **Online Certification Authority** window, in the **Specify Online Certification Authority** box, select the **Domain Certificate** and click **OK**.
- 11 Enter a user friendly name such as **HTTPS** and click **Finish**.
- 12 Go to **Default Web Site** on the IIS Manager and right click.
- 13 Select **Bindings** on the menu options.

- 14 In the **Site Bindings** window, click **Add**. The **Add Site Binding** window is displayed.
 - a Select **https** under **Type**.
 - b The default **Port** number is displayed as **443**. Leave the default port number.
 - c Under **SSL certificate**, select the SSL certificate that you have downloaded for the system. For more information on creating an SSL certificate, see Microsoft KB article 228991 available at <http://support.microsoft.com/kb/228991>.
 - d Click **OK**.
- 15 Confirm the IIS installation by typing **https://localhost** in your browser.

Discovery Settings for the WCM Server

When the WCM client starts after log in it searches network services (DNS and DHCP) for an FTP/HTTP/HTTPS server to download the file, or uses a locally available file on the device. The process by which the configuration files are obtained by the WCM agent on the thin client is in the following order:

- 1 DNS Service Record Lookup
- 2 DNS Hostname Lookup
- 3 DHCP Option Tags

DNS Service Record Lookup

The DNS Service Record Lookup method (also known as SRV record) obtains information about the WCM Repository Server and the configurations that utilize DNS. For example, the information and parameters are obtained from a DNS server. The method uses a Uniform Resource Locator (URL) for this purpose. For example, a URL obtained from the DNS server. Due to the restrictions on the data that can be specified for DNS service record and a DNS hostname record, it is assumed that the authentication (username/log in) used on the Repository Server is **Anonymous**.

In the DNS service record lookup, an administrator can configure the DNS server to provide the server and port number for a service that is referred to as `_WCM._tcp`. Multiple configuration repository server/port values can be provided. The WCM agent accesses them in order, according to the weight and priority associated with each entry.

Since the DNS server may not supply a protocol string associated with each server/port entry, the WCM agent determines the protocol based on the port specified. For example, if port 80 is specified, the WCM agent determines that the protocol being used is HTTP. If the DNS service record lookup for `_WCM._tcp <full domain>` fails, the WCM agent attempts `_WCM._tcp <sub-domain>` and so on upon further failures. For example, if the domain name is x.y.z, the WCM agent issues a DNS service location lookup using the following names in the order shown until the DNS server returns a valid answer:

- 1 `_ WCM._tcp.x.y.z`
- 2 `_ WCM._tcp.y.z`
- 3 `_ WCM._tcp.z`

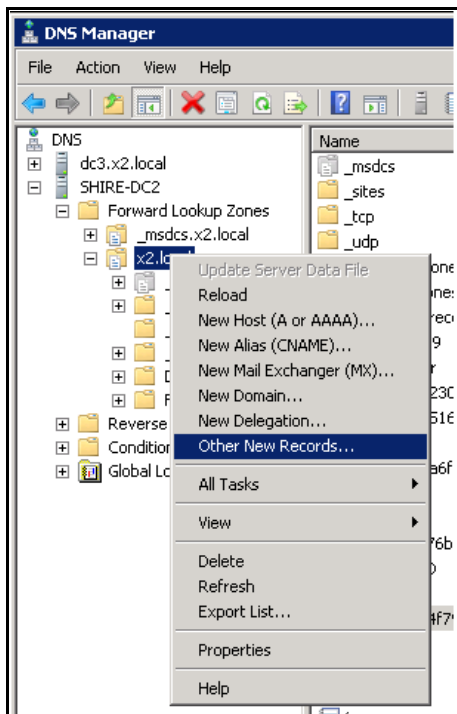
Configuring the DNS Service Lookup

For more information on installing DNS on a Windows 2003 Server, go to <http://support.microsoft.com/kb/814591>.

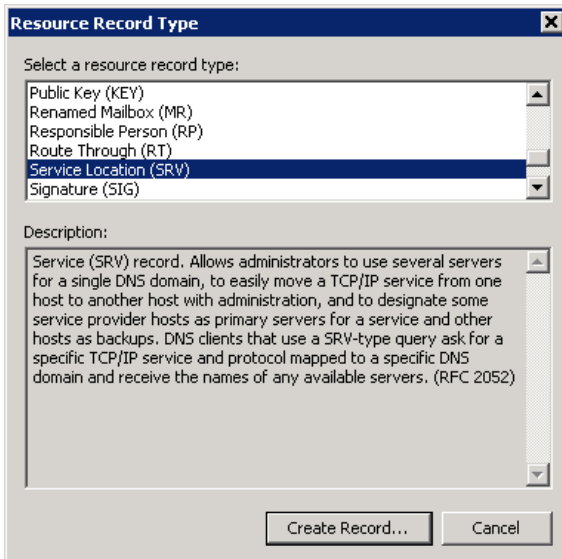
For more information on installing DNS on a Windows 2008 Server, go to <http://technet.microsoft.com/en-us/library/cc725925.aspx>.

To configure the DNS Service (SRV) lookup:

- 1 Open the DNS Manager after installing the DNS Server.
- 2 Under the **Domain**, right click and select **Other New Records**.



- 3 In the **Resource Record Type** dialog box, select **SRV Location** and click **Create Record**.



- 4 In the **New Resource Record** dialog box, enter the following values:
- **Service Name** – `_WCM`
 - **Protocol** – `_tcp`
 - **Port Number** – either 21, 80, or 443 depending on whether you choose FTP, HTTP, or HTTPS protocols.
 - **Host Offering this Service** – enter the hostname of the repository server.

New Resource Record

Service Location (SRV)

Domain: x2.local

Service: _WCM

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 21

Host offering this service: wcmserver.x2.local

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

5 Click OK.

DNS Hostname Lookup

If the WCM agent is unable to obtain a valid answer to DNS service record lookup requests, it then attempts a DNS Hostname lookup.

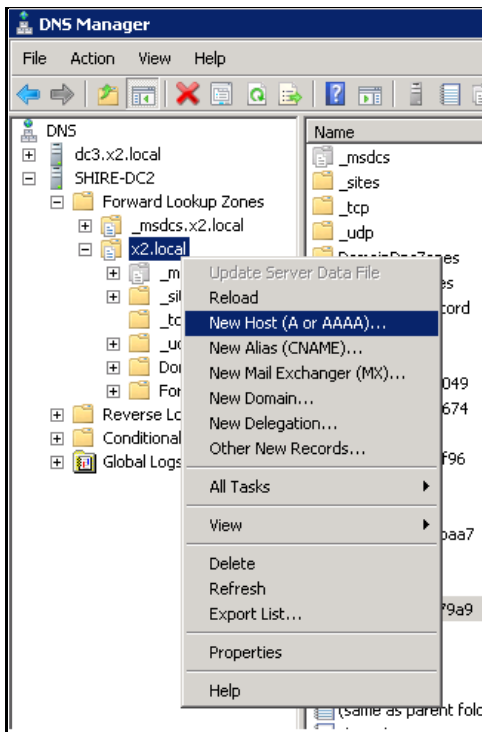
An administrator can configure the DNS server to provide the server IP for a host name. With the DNS Hostname record it is not possible to supply protocol or port. Therefore, the retrieval module first uses the HTTPS on port 443. If this fails, the WCM agent then uses the HTTP on port 80. If the lookup for host name WCM in the client's domain fails, the WCM agent then attempts to look for WCM for each sub-domain name. For example, if the domain name is x.y.z, the WCM agent issues a DNS host name lookup using the following names in the order shown until the DNS server returns a valid answer:

- 1 WCM.x.y.z
- 2 WCM.y.z
- 3 WCM.z

Configuring the DNS Hostname

To configure the DNS Hostname:

- 1 Under **DNS Host**, select **New Host**. The **New Host** dialog box is displayed.



- 2 In the **New Host** dialog box, enter **wcm** under **Name** and provide the IP address of the IIS Server.

3 Click **Add Host**.

DHCP Option Tags Lookup

When configuring the DHCP server for use with WCM, use the DHCP option tags listed in Table 2-1.

Ensure that the DHCP option tags that you create are activated within the DHCP scope. This can be done using the **Scope Options** dialog box on the DHCP server (after you add them) or the **Configure Options** command (before you add them). For details on your network environment and DHCP layout, contact your network administrator.

Table 2-1. DHCP Option Tags

Option Tag	Description	Examples of Values to Use
6	Domain Name Server (DNS). Optional, but recommended. Can be either an IP address or a string .	IP Address example: 192.168.1.20 String example: MyDNSServer.com

Table 2-1. DHCP Option Tags

Option Tag	Description	Examples of Values to Use
183	Defines protocol to be used for downloading the configuration file to the client and any custom items in the folder from the server specified in DHCP Option 195 . Valid protocols are FTP, HTTP, and HTTPS. The default protocol is FTP.	Use only one of the following values: <ul style="list-style-type: none"> • FTP example: FTP • HTTP example: HTTP • HTTPS example: HTTPS
184	Server username. Optional string. This is the username to use when authenticating to the server specified in Option 195 .	String example: MyServerUsername
185	Server Password. Optional string. Password to use when authenticating to the server specified in Option 195 . If the server allows Anonymous log in, you can leave this option blank.	String example: MyServerPassword
195	Server (ftp/http/https). Optional IP Address or string. Can be either the IP Address or the fully qualified domain name (FQDN) of the Repository server. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to be the server.	IP Address example: 192.168.100.7 String example: MyServer.com

Table 2-1. DHCP Option Tags

Option Tag	Description	Examples of Values to Use
196	<p>Default configuration path (ftp/http/https). Optional string. The relative directory starting from the root directory must be given. If 196 is not defined and is left blank:</p> <ul style="list-style-type: none">• FTP: For FTP, the default configuration path is C:\inetpub\ftproot\Wyse\WES7.• HTTP or HTTPS: For HTTP or HTTPS, the default configuration path is the path specified by the virtual directory in IIS; usually wwwroot. For example, C:\inetpub\wwwroot\Wyse\WES7.	<p>For custom configuration paths use only one of the following string values where <i>Finance</i> is your custom defined path for DHCP Option 196:</p> <p>FTP custom example: C:\inetpub\ftproot\Wyse\WES7\Finance</p> <p>HTTP custom example: C:\inetpub\ftproot\Wyse\WES7\Finance</p> <p>HTTPS custom example: C:\inetpub\ftproot\Wyse\WES7\Finance</p>

Configuring DHCP Options

On the DHCP server, you need to add three Wyse vendor tags – 183, 195 & 196. Option Tag 183 defines the protocol to use with WCM. Valid protocols are FTP, HTTP, and HTTPS. Option Tag 195 identifies the IP address of the FTP server that the thin client system connects to. Option Tag 196 contains the directory details of the configuration file that the thin client system downloads.

Configuring DHCP Options on a Windows 2003 Server

- 1 Right-click **My Computer** and select **Manage**.
- 2 Expand **Services and Applications**.
- 3 Highlight **DHCP** and click **Set Predefined Options**.

The **Predefined Options and Values** screen is displayed.

- 4 Click **Add** to add an option in the **Option Type** window.
- 5 Add the following details one at a time in the **Option Type** window:

Table 2-2. DHCP Options

Name	Data Type	Code	Description
DNS Server	String	6	DNS Server
WCM Protocol	String	183	WCM Protocol
WCM Server Username	String	184	WCM Server Username
WCM Server Password	String	185	WCM Server Password
WCM Server	String	195	WCM Server
WCM Path	String	196	WCM Path

- 6 On the **Predefined Options and Values** screen, scroll down to verify that the options have been added.
- 7 Select option tag **6** and enter the IP address of the DNS Server or the name of the DNS Server.
- 8 Select option tag **183**, and enter the protocol you will be using on your server.
- 9 Select option tag **195** and enter the IP address of your FTP, HTTP or HTTPS server that contains the WCM configuration files and press **OK**.
- 10 Select option tag **196** and enter the string “/ ” (forward slash) and press **OK**. This sets the default path to ftproot/wyse/wes7 directory if you are using FTP as the protocol or webroot/wyse/wes7 if using HTTP or HTTPS as the protocol.
- 11 Select option tag **184** and enter the username to use when authenticating to the server specified in step 9 (option tag 195). If the server allows Anonymous log in, you can enter the value **Anonymous**.
- 12 Select option tag **185** and enter the password to use when authenticating to the server specified in step 9 (option tag 195). If the server allows Anonymous log in, leave this field blank.

- 13 Add the options to the DHCP scope. Navigate back to **DHCP** in the Computer Management screen, right click **Scope Options** and select **Configure Options**.
- 14 Ensure to select options 183, 195, and 196. Press **OK** to save and exit.

Configuring DHCP Options on a Windows 2008 Server

- 1 Launch **Server Manager** from the **Start** menu.
- 2 Under **Roles**, expand the **DHCP Server**, select your server and expand it.
- 3 Select **IPv4** and expand it.
- 4 Right click **Scope Options** and select **Configure Options**. The Scope Options window is displayed.
- 5 Select option tag **6** and enter the IP address of the DNS Server or the name of the DNS Server.
- 6 Select option tag **183**, and enter the protocol that you want to use on your server.
- 7 Select option tag **195** and enter the IP address of your FTP, HTTP or HTTPS server that contains the WCM configuration files and click **OK**.
- 8 Select option tag **196** and enter the string **"/ "** (forward slash) and click **OK**. This sets the default path to the **ftproot/wyse/wes7** directory if using FTP as the protocol or **webroot/wyse/wes7** if using HTTP or HTTPS as the protocol.
- 9 Select option tag **184** and enter the username to use when authenticating to the server specified in step 9 (option tag 195). If the server allows Anonymous log in, enter the value **Anonymous**.
- 10 Select option tag **185** and enter the password to use when authenticating to the server specified in step 9 (option tag 195). If the server allows Anonymous log in, leave this field blank.
- 11 Click **OK**.

Configuring the WCM Thin Client Systems

To manually configure the DHCP options on thin client systems:

- 1 Log in as Administrator into the thin client systems and launch the WCM from the Control Panel.

2 Click **Advanced Options** and set the following values:

- **Server** – The default DHCP option is 195. This is the server IP Address or the fully qualified domain name (FQDN) of the server.
- **Path** – The default DHCP option is 196. This is the root path to the server; ftp, http, or https.
- **Username** – (Optional) The default DHCP option is 184. This is the server username of the server specified in DHCP option 195.
- **Password** – The default DHCP option is 185. This is the password of the server specified in DHCP option 195. If the server allows Anonymous log in, leave this option blank.
- **Protocol** – The default DHCP option is 183. This is the protocol (ftp/http/https) used for downloading the configuration file (and any custom items in the folder) from the server specified in DHCP option 195 (the default protocol is FTP)

3 Click **Save Settings**.



NOTE: You must ensure that the DHCP options that you specify in the thin client systems are identical to the options specified in the DHCP server. This is needed for the discovery of the thin clients by the Repository Server.

Configuring the Dell Wyse Device Manager (WDM) Server

If you are using the WDM Server to push the configuration files to the thin clients, you need to edit the **WES_ApplyConf.rsp**, **WES7_ApplyConf.rsp**, or **WE8S_ApplyConf.rsp** files for the WES2009, WES7 or WE8S thin client systems respectively.

There are two ways in which you can push the configuration files to the thin clients:

- **Through the Remote Path (RP) Command** — This method sets the repository path to that of WDM server and the thin client system picks up the latest configuration from this path on every log in.
- **Through the Apply Configuration (AC) Command** — This method enables the thin client system to download the configuration file from the WDM server and apply it on every log in.

To register the **RP Command** package in the WDM server:

- 1 Create an XML file from the WCM Application GUI by enabling the **Use WDM** option under **Agent Settings**.
- 2 Log in to the WDM Server system as an Administrator.
- 3 Place the XML file in the **RP Command** folder. For example, **C:\Program Files\WDM\WDM_WCM\RP Command\TestRP_WES\Wyse\WES\WESConfig.xml**.
- 4 Register the **.rsp** package in the WDM server and apply it on the thin client system.
- 5 Restart the thin client system for the changes to take effect. You will notice that the **Remote/WDM** option in the **Import Configuration** screen of the WCM Client is disabled and populated with the WDM server details.

To register the **AC Command**:

- 1 Create an XML file from the WCM Application GUI by editing any of the existing XML files.
- 2 Open the XML file in a text editor and change the **<uiProtocol>** tag to **<uiProtocol> local</uiProtocol>**. Save the file.
- 3 Log in to the WDM Server system as an Administrator.
- 4 Place the XML file in the AC Command folder. For example, **C:\Program Files\WDM\WDM_WCM\AC Command\WES7_AC\WES7_AC\temp\WES7Config.xml**.
- 5 Open the **WES_ApplyConf.rsp**, **WES7_ApplyConf.rsp**, or **WE8S_ApplyConf.rsp** file from the location where you have installed WDM in a text editor. For example, **C:\Program Files\WDM\WDM_WCM\WES_ApplyConf\WES_ApplyConf.rsp**.
- 6 Under the **Copy over new files** section, enter the location of the configuration XML file against the AC command. For example: **AC "C:\temp\WES7Config.xml"**. This is the local path on the thin client system to which the configuration file gets downloaded.
- 7 Save and close the file.

Your WDM server is now configured to push the configuration files to the thin clients. You also need to configure the **Agent Settings** in the WCM Application GUI to complete the setup. For more information, see [Agent Settings](#). For more information on registering a **.rsp** package, see the *WDM Administrator's Guide*.

Using the Dell Wyse Configuration Manager (WCM) GUI Application

This chapter discusses in detail how to use the WCM GUI Application that is installed on the Repository Server. You can create configuration files, edit existing configuration files, and save the configuration files in a central location. The thin client system connects to the central location and downloads the respective configurations.

About the WCM Application GUI

The WCM Application GUI is installed and available on the repository server. You must log in to the repository server as the administrator to launch and access the WCM Application GUI. The GUI consists of the following components:

- **Configuration Explorer** — Contains the **Configurations** tab that consists of the names of the areas you can configure for your configuration files. The names of the areas that you can configure are displayed as a tree structure with the main areas as the main nodes and the sub-areas as sub-nodes.
- **Toolbar** — Contains icons that are located on top of the **Configurations** tab and can be used for the main nodes and sub-nodes in the **Configurations** tab. Each icon has a tool-tip description for easy identification.
- **Right-click Menus** — Provides easy access to perform the various tasks. You can right-click certain items on the **Configurations** tab to view the menu of the available tasks.
- **Details Pane** — Displays the detailed configuration settings for the selected nodes and sub-nodes in the **Configurations** tab on the right pane of the GUI. You can modify these settings to create a new configuration file or edit an existing configuration file.
- **Menu Bar** — Provides the various menu options for you to effectively use the WCM Application GUI.

Table 3-1. Menu Options

Option Name	Description
New	<p>You can select the operating system you want to use with your new configuration file from this option. You can select from the following options:</p> <ul style="list-style-type: none">• Windows Embedded Standard 8 (WE8S)• Windows Embedded Standard 7 (WES7)• Windows Embedded Standard (WES 2009)
Open	<p>You can use this option to load an existing configuration file to make modifications.</p>
Save	<p>You can use the Save or Save As functions to save the configuration files.</p>
Options	<p>This has the following sub-options:</p> <ul style="list-style-type: none">• Append Settings – You can use this to switch Append Settings on (checked) and off (cleared). When Append Settings is ON (default setting), the settings of the configuration file that you are not changing are retained from the last saved configuration, and only the new changes get appended. When Append Settings is OFF, the settings of the configuration file that you are not changing are set back to the default values.• Agent Settings – You can click this to open and use the Agent Settings dialog box to configure your default client agent settings. <p>For more information, see Agent Settings.</p>
Help	<p>You can use this to open Help and the About Dell Wyse Configuration Manager dialog box displaying the software version.</p>

Creating New Configuration Files

You can use the WCM Application GUI to create new configuration files to be applied to thin clients.

To create new configuration files:

- 1 Log in to the repository server or the system where you have installed WCM and launch the WCM Application GUI.
- 2 Click one of the following options to create a new configuration file:
 - New Windows Embedded Standard 8 Configuration (WE8S)
 - New Windows Embedded Standard 7 Configuration (WES7)
 - New Windows Embedded Standard Configuration (WES2009)

You can also choose the preceding options from the **New** menu.

- 3 In the **Configurations** tab, check the options that you need to configure and provide the corresponding values in the **Details** pane.

For more information, see [Configuration Details](#).

- 4 After providing the **Configuration** details, click the Save menu and enter a name for the configuration file.

The path where the file is saved is dependent on the option you choose in [step 1](#) and the protocol you have chosen for the file transfer.

If you are using the Repository Server for automatic upgrades, then the default folder locations are:

- **For FTP:**
 - C:\inetpub\ftproot\Wyse\WES\WESConfig.xml
 - C:\inetpub\ftproot\Wyse\WES7\WES7Config.xml
 - C:\inetpub\ftproot\Wyse\WE8S\WE8SConfig.xml
- **For HTTP/HTTPS:**
 - C:\inetpub\ftproot\Wyse\WES\WESConfig.xml
 - C:\inetpub\ftproot\Wyse\WES7\WES7Config.xml
 - C:\inetpub\ftproot\Wyse\WE8S\WE8SConfig.xml



NOTE: The required names for each of the configuration files for each platform should be WE8S - WE8SConfig.xml, WES7 - WES7Config.xml, and WES2009 - WES2009Config.xml respectively. If the thin client system is a domain user, then the name of the configuration file should be **administrator.xml** to enable the domain user client systems to download the configurations.

If you are using the WCM Client to import the files, then you can save the configuration files in a local or remote folder location that is easily accessible by the thin clients.

Editing Existing Configuration Files

To edit an existing configuration file:

- 1 Launch the WCM Application GUI and click the **Open an Existing Configuration** option in the Details pane. You can also click the **Open** menu to open an existing configuration file.
- 2 Navigate to the location to select your configuration file. For more information on the default location, see [step 4](#) in [Creating New Configuration Files](#).
- 3 Modify the configuration details and click the **Save** menu to save the file. You can choose to save the file with the same name or with a different name.

Configuration Details

You need to configure the various configuration areas to create or modify the configuration files to be deployed on the thin client systems.

The **Configurations** tab on the WCM Application GUI displays the configuration areas with the corresponding details on the **Details** pane. The configuration areas are broadly classified as:

- [Connections](#)
- [Device Configuration](#)
- [OS Configuration](#)

To enter configuration details:

- 1 Select the configuration area in the **Configurations** tab, and enter the values in the **Details** pane for the selected area.

When you select any of the details in the **Details** pane, the corresponding description is displayed at the bottom of the screen.

- 2 After you enter the values for the details, ensure that you click **Apply Changes** to save your changes.
- 3 Click **Discard Changes** to reset the values back to the defaults.



NOTE: If you use a server environment (FTP, HTTP, or HTTPS) and intend to create configuration files that thin clients can access automatically to update themselves, ensure to name your file WESConfig.xml for WES2009, or WES7Config.xml for WES7/WES7p, or WE8SConfig.xml for WE8S and place the file into the correct folder according to the protocol you use. If the thin client system is a domain user, then the name of the configuration file should be **administrator.xml** to enable the domain user client systems to download the configurations.

Connections

The Connections area enables you to set the configurations for the different types of connections that the thin client can use to connect to the servers. This area consists of:

- **RDP** — to configure the remote desktop protocol settings to connect to any remote computer.
- **VMware View** — to configure the VMware View client to connect to the VMware View Connection Server.
- **Citrix** — to configure the Citrix client to connect to the Citrix server.
- **vWorkspace** — to configure the vWorkspace to connect to any Quest vWorkspace server in your environment.

RDP

The RDP settings are grouped under Basic Settings, Display, Local Resources, Other RDP Settings, and Unrecognized Settings.

Table 3-2. RDP Details

RDP Setting	Description	Expected Value
Basic Settings		
Autostart	Starts the RDP connection automatically when you log in to the thin client.	True or False.
Connection Name	Name of the Desktop shortcut for the connection. This is mandatory.	Enter any name here.
Domain Name	Name of the domain to which the thin client connects. This is optional.	Enter the domain name.
Host Name or IP Address	Host name or the IP address of the remote computer. This is optional.	Enter the host name or the IP address of the remote computer.
User Name	User name to be used for connecting to the RDP session. This is optional.	Enter a user name.
Password	Password to be used for connecting to the RDP session. This is optional.	Enter the password.
Single Sign On	Enables single sign-on for domain joined devices. You can use this feature to connect such devices using RDP, VMware View or Citrix.	True or False.
Display		
Display Connection Bar	Display a connection bar at the top of the screen in the full-screen mode.	True or False.
Multi-Monitor Support	Enable multiple-monitor support for the connection.	True or False.
RDP Window Screen Size	Size of the RDP screen on the host system.	Select an option from the drop-down list.

Table 3-2. RDP Details *(continued)*

RDP Setting	Description	Expected Value
Screen Color Depth (in bits)	The color depth and quality of the connection.	Select an option from the drop-down list.
Screen Mode Type	The remote connection window mode.	Select an option from the drop-down list.
Local Resources		
Redirect Clipboard	Enables the local clipboard on the thin client device to be used in the remote connection.	True or False.
Redirect COM Ports	Enables the local COM ports to be used in the remote connection.	True or False.
Redirect DirectX	Determines whether the DirectX on the client system is redirected and available in the remote session when you connect to a remote computer by using the Remote Desktop Connection (RDC).	True or False.
Redirect Drives	Enables the local drives of the thin client device to be used in the remote connection.	True or False.
Redirect POS Devices	Enables the Point of Service (POS) devices such as bar code scanners or magnetic readers that are attached to the thin client device, to be used in the remote connection.	True or False.
Redirect Printer	Enables the printer attached to the thin client device to be used in the remote connection.	True or False.

Table 3-2. RDP Details *(continued)*

RDP Setting	Description	Expected Value
Redirect Smart Card	Enables the smart cards attached to the local device to be used in the remote connection.	True or False.
Other RDP Settings	<p>Allows you to set up the following details:</p> <ul style="list-style-type: none"> • Local and Program – includes remote audio and keyboard settings, programs that start up on connection, prompt for credentials, negotiate security layer, enable compression, and enable video playback options • Experience – includes performance options and other desktop features to be enabled. • Advanced – includes server details and remote desktop gateway settings. 	Click Apply Changes to save the changes.
Unrecognized Settings	If you have created specific configuration settings in a reference thin client system and exported the configuration file to the Repository Server, and you open that configuration file, the Application GUI displays the settings as unrecognized settings.	The Application GUI preserves the original settings without any changes when you save the configuration file.

VMware View

The VMware View details are grouped under Basic Settings and Advanced Settings.

Table 3-3. VMware View Details

VMware View Setting	Description	Expected Value
Basic Settings		
AutoStart	Starts the connection automatically when you log in to the thin client.	True or False.
Desktop Name	The desktop pool name in the View Connection Server. This is optional.	Enter the name.
Display View Bar	Enable or disable the display of the VMware View menu bar in full-screen mode. This is optional.	True or False.
Server URL	The View Connection Server hostname or IP address. This is required.	Enter the server URL or the IP address.
Domain	The domain where the View Connection Server is located. This is optional.	Enter the domain name
User Name	Log in name of the user for the View Connection Server. This is optional.	Enter the user name.
Password	Password of the log in user for the View Connection Server. This is optional.	Enter the password.
Advanced Settings		
Auto Connect	This re-establishes the connection to the View Connection Server. This is optional.	True or False.

Table 3-3. VMware View Details *(continued)*

VMware View Setting	Description	Expected Value
Broker	The hostname or the IP address of the View Connection Broker. This is optional.	Enter the hostname or IP address.
Broker History	The alternate or previously used View Connection Broker hostname or IP address. This is optional.	Enter the previously used hostname or IP address.
Desktop Protocol	The protocol used by the VMware View client for the connection.	Select an option from the drop-down list.
Login as Current User	Enable log in to the View Connection Server with the Windows log in credentials of the thin client device. This now enables the single sign-on feature and you can use this feature to connect to domain joined devices using RDP, VMware View or Citrix.	True or False.
Screen Size	The screen size of the View Connection Server window. This is optional.	Select an option from the drop-down list.
SSL Configuration	Determines how the client connects if it cannot verify a secure connection to the server. A secure connection requires that the server URL begins with https:// and a certificate on the client.	Select an option from the drop-down list.

Citrix

The Citrix client details are grouped under Basic Settings and Advanced Settings.

Table 3-4. Citrix Client Details

Citrix Setting	Description	Expected Value
Basic Settings		
Autostart	Automatically starts the connection when you log in to the thin client.	True or False.
Citrix Server	The host name or the IP address of the Citrix server. This is mandatory.	Enter the hostname or IP address.
Domain Name	The name of the domain where the Citrix server is hosted. This is optional.	Enter the domain name.
User Name	The user name to connect to the Citrix session. This is optional.	Enter the user name.
Password	The password to connect to the Citrix session. This is optional.	Enter the password.
Launch Application	The default application to be launched after logging in. This is optional.	Enter the name of the application.
Published Server Type	The Citrix server type that is used for appliance mode connections. This is optional.	Select an option from the drop-down list.
Single Sign-on	Enables single sign-on for domain joined devices. You can use this feature to connect such devices using RDP, VMware View or Citrix.	True or False.
Application Display		

Table 3-4. Citrix Client Details *(continued)*

Citrix Setting	Description	Expected Value
Desktop Display	Displays the Citrix connection on your desktop. This is optional.	True or False.
Desktop Folder Name	The folder name on the desktop. This is optional.	Enter a folder name.
Start Menu Display	Enables the start menu display.	True or False.
Start Menu Display Folder	The folder on the Windows start menu where the Citrix connection is added.	Enter the folder location.
System Tray Display	Displays the Citrix connection icon in the system tray.	True or False.
Flash Player Redirection Settings		
Use Flash Remoting	Enables HDX MediaStream Flash redirection on the thin clients.	Select an option from the drop-down list.
Enable Server Side Content Fetching	Enabling this setting causes the Flash content to be downloaded to the server and then transmitted to the thin clients.	Select an option from the drop-down list.
Use Server HTTP Cookies	Enables synchronization of the client-side HTTP cookies with the server-side to download HTTP cookies from the server.	Enable or Disable.
URL Rewriting Rules for Client-side Content Fetching	Rules to redirect the user devices to other servers for client-side content fetching.	Click to launch the Rule Window to enter the URL rewriting rules. After you enter the rules, they are separated by a semi colon and the rule name and description are separated by a colon.

Table 3-4. Citrix Client Details *(continued)*

Citrix Setting	Description	Expected Value
Server Options		
Logon Methods	The logon method to connect to the Citrix Server. This is optional.	Select an option from the drop-down list. The Default Logon Method option uses the method configured on the Citrix server. The Prompt User option prompts you to enter the log in credentials to connect to the Citrix server.
Session Options		
Audio Quality	The audio quality for the connection that controls the multimedia bandwidth. This is optional.	Select an option from the drop-down list.
Color Depth	The color quality of the display for the connection. This is optional.	Select an option from the drop-down list.
Display Dimensions	The display resolution of the remote connection. This is optional.	Select an option from the drop-down list.
Advanced Settings		
Automatic Reconnection at Logon	Automatically reconnect to existing sessions upon log on.	True or False.
Logon - Connect to Active and Disconnected Sessions	Connect to active and disconnected sessions upon logon if set to True . Connect to only disconnected sessions upon logon if set to False .	True or False.

Table 3-4. Citrix Client Details *(continued)*

Citrix Setting	Description	Expected Value
Menu - Connect to Active and Disconnected Sessions	Connect to active and disconnected sessions upon logon if set to True and provide the menu.	True or False.
Reconnect from Menu	Reconnect to existing sessions from the client menu.	True or False.
User Key Combos Passthrough	To apply the Windows user key combinations of a window.	Select an option from the drop-down list.

vWorkspace

The vWorkspace details are listed under Basic Settings.

Table 3-5. vWorkspace Details

vWorkspace Setting	Description	Expected Value
Basic Settings		
Autostart	Starts the vWorkspace connection automatically when you log in to the thin client.	True or False. NOTE: If you set this value to True , you cannot set the Appliance mode on for vWorkspace or any of the other options.
Configuration File Location	Location of the Quest vWorkspace configuration XML file. It could be on the local system or a remote system.	Local or Remote.

Table 3-5. vWorkspace Details *(continued)*

vWorkspace Setting	Description	Expected Value
Connection(s)	Full path or the URL where the Quest vWorkspace configuration file is located.	<p>If you select Local, then enter the location of the vWorkspace configuration XML file on the local machine</p> <p>If you select Remote, then enter the complete URL(s) location of the Quest vWorkspace configuration XML file location on the remote vWorkspace server.</p> <p>NOTE: You can enter multiple Remote XML file locations but only one Local location.</p>



NOTE: You can use the existing Quest vWorkspace configuration XML file or create it using the Quest vWorkspace AppPortal installed on any system.

Device Configuration

The Device Configuration area enables you to set the configurations for the hardware connected to or located on the thin client devices.

This area includes:

- **Display** — to configure the display settings.
- **Mouse** — to configure the mouse settings.
- **Keyboard** — to configure the keyboard settings.
- **Share - New Share** — to configure the share drives and create new file share locations.
- **Timezone** — to configure the timezone.
- **Ethernet** — to configure the ethernet settings.
- **Wireless Profile** — to configure wireless profiles.

- **Audio** — to configure audio settings.
- **Power** — to configure power settings.

Display

Table 3-6. Display Setting Details

Display Setting Name	Description	Expected Value
Multi-Monitor Settings		
Multiple Displays	If the device has multiple display units attached to it, you can configure the options.	Select an option from the drop-down list.
Desktop Color Settings		
Desktop Color	The background color of the thin client's local desktop.	Click the arrow to enter the custom, web, or system color from the color bars.
Desktop Wallpaper Settings		
Desktop Wallpaper	Path and name of the wallpaper image file.	Navigate to the location of the image file and enter it. NOTE: WES2009 thin client systems support only .bmp type images for their desktop background and not .jpg type images.
Desktop Wallpaper Layout	Layout of the desktop wallpaper.	Select an option from the drop-down list.
Monitor1 and Monitor2 Display Settings		
NOTE: Monitor2 display settings are applicable only if there are multiple monitors attached to the device.		
Default Display Configuration	The default configuration for resolution, refresh rate, and color depth.	True or False.
Color Depth (bits)	Quality of the display.	Select an option from the drop-down list.

Table 3-6. Display Setting Details *(continued)*

Display Setting Name	Description	Expected Value
Display Orientation	Orientation of the thin client system's display.	Select from Portrait or Landscape.
Display Position	Position of the display on the first monitor relative to display on the other monitor.	Select an option from the drop-down list.
Display Resolution	Screen resolution of the display.	Select an option from the drop-down list.
Is Primary Display	If the monitor is used as a primary display.	True or False.
Refresh Rate (Hz)	Refresh rate of the display.	Select an option from the drop-down list.

Mouse

Table 3-7. Mouse Setting Details

Mouse Setting Name	Description	Expected Value
Basic Mouse Settings		
Click Lock	Enables you to highlight or drag without holding down the mouse button.	True or False.
Click Lock Time	The duration for which the mouse or trackball button should be held down before the click is locked.	Click the arrow and adjust the timing on the scale provided.
Double Click Speed	The speed with which you double click the mouse.	Click the arrow and adjust the speed on the scale provided.
Right Click as Primary	Set the right click as the primary option.	True or False.
Mouse Pointer Options		

Table 3-7. Mouse Setting Details *(continued)*

Mouse Setting Name	Description	Expected Value
Find Mouse Pointer	To show the location of the mouse pointer when the CTRL key is pressed.	True or False.
Hide Mouse Pointer	To hide the location of the mouse pointer when the CTRL key is pressed.	True or False.
Mouse Pointer Speed	The speed of the mouse pointer.	Click the arrow and adjust the speed on the scale provided.
Pointer Trail Length	The length of the pointer trail.	Click the arrow and adjust the length of the trailer on the scale provided.
Snap Mouse Pointer	To automatically move the mouse pointer to the default button in a dialog box.	True or False.
Mouse Vertical Scrolling		
Scroll Lines	The number of lines scrolled at a time using vetical scrolling.	Click the arrow and adjust the number on the scale provided.

Keyboard

Table 3-8. Keyboard Setting Details

Keyboard Setting Name	Description	Expected Value
Keyboard Options		
Blink Rate	The cursor blink rate.	Click the down arrow and adjust the blink rate on the scale provided.
Input Languages	The input language for the keyboard.	Select an option from the drop-down list.
Keyboard Layout	The layout and language of the keyboard according to the language selected.	Select an option from the drop-down list. This should be the same as the input language you have selected.

Table 3-8. Keyboard Setting Details *(continued)*

Keyboard Setting Name	Description	Expected Value
Keyboard Preferences	Enables you to set keyboard hotkeys.	True or False.
Keyboard Repeat Delay	The duration for which a key can be pressed without the letter being repeated as an input.	Select an option from the drop-down list.
Keyboard Repeat Rate	The rate at which a keyboard character repeats.	Click the down arrow and adjust the repeat rate on the scale provided.
Menu Access	Allows you to enable menu access keys on the keyboard.	True or False.

Share - New Share

Table 3-9. New Share Details

New Share Setting Name	Description	Expected Value
Share		
Share Name	Shared drive alphabet. For example, Y or S .	Enter a drive letter suitable to your network.
Remote Path	The path of the shared drive on the server. For example, \\Server\Share if it is the same domain. If the server is on a different domain, then enter the path as Domain\User Name .	Enter the complete path of the shared drive.
User Name	User name to connect to the share.	Enter the user name.
Password	Password to connect to the share.	Enter the password.

Timezone

Table 3-10. Timezone Details

Timezone Setting Name	Description	Expected Value
Timezone Options		
Timezone Name	Timezone of the thin client device.	Select a timezone from the drop-down list.
Bias	The difference in minutes between Co-ordinated Universal Time (UTC) and Local Time.	Automatically populated after you select the timezone.
Daylight Bias	The difference in minutes that the clock changes at the daylight saving time start date.	Automatically populated after you select the timezone.
Standard Bias	The difference in minutes that the time zone is offset from the UTC.	Automatically populated after you select the timezone.
Supports Daylight Savings	Specifies if daylight savings is supported by the selected timezone.	Automatically populated after you select the timezone.
Time Server	The server that reads the actual time from a reference clock and distributes this information to the thin client devices. The time server may be a local network time server or an internet time server.	Enter the name of the time server.
Timezone Keyname	The name of the selected timezone.	Automatically populated after you select the timezone.
Disable Dynamic Daylight Time	To disable daylight savings if the selected timezone supports daylight savings.	True or False.

Ethernet

Table 3-11. Ethernet Details

Ethernet Setting Name	Description	Expected Value
DHCP Settings		
Enable DHCP	To assign an IP address from a DHCP server. If set to False, you must enter a static IP address.	True or False.
Static IP Settings		
IP Address	A specific or static IP address for the thin client device. This is mandatory if you set the Enable DHCP to False.	Enter an IP address.
Gateway Address	The IP address of the routing gateway for the thin client device.	Enter the IP address.
Subnet Address	The subnet address for the static IP address of the thin client device.	Enter the subnet address.
DNS Addresses		
DNS1 Address	IP address of the primary DNS server of the thin client device.	Enter the IP of the primary DNS server.
DNS2 Address	IP address of the secondary DNS server of the thin client device.	Enter the IP of the secondary DNS server.
WINS Addresses		
WINS1 Address	IP address of the primary WINS server of the thin client device.	Enter the IP of the primary WINS server.
WINS2 Address	IP address of the secondary WINS server of the thin client device.	Enter the IP of the secondary WINS server.

Wireless Profile

Table 3-12. Profile Details

Profile Setting Name	Description	Expected Value
General Settings		
Make Current Profile Active	To set the current profile active.	True or False.
Radio State	To change the WiFi radio state.	On or Off.
WLAN Profile		
Connect to a Hidden Network	To connect to a network that does not broadcast its SSID.	True or False.
Connection Mode	To connect automatically or let the user connect manually.	Auto or Manual.
Profile Name	Name of the wireless profile.	Enter a name for the profile.
SSID Name	The Service Set Identifier of the WiFi Network.	Enter the SSID name.
WLAN Connection Type	The WLAN connection type.	Enter whether it is an independent/ad-hoc WiFi network (IBSS) or multiple WiFi AP's working as a single network. (ESS).
Security		
Authentication	Authentication method required for connecting to the WiFi network.	Select an option from the drop-down list.
Encryption	Data encryption method used to send the data over the WiFi network.	Select an option from the drop-down list.
Key Phrase	Network password or key. This is required if encryption and authentication are enabled.	Enter a value for the key.

Table 3-12. Profile Details *(continued)*

Profile Setting Name	Description	Expected Value
Key Type	The element that indicates whether the shared key is a network key or a pass phrase.	Network Key or Pass Phrase.
Shared Key Encrypted	The protected element that indicates whether a shared key is encrypted.	True or False. Set this property to True only if you are going to enter the password.
Use IEEE 802.1X	This element indicates whether 802.1X authentication is used.	True or False.

Audio

Table 3-13. Audio Details

Audio Setting Name	Description	Expected Value
Audio Settings		
Mute MIC	To mute the microphone on the thin client device.	True or False.
Mute Speakers	To mute the speakers on the thin client device.	True or False.
Set MIC Volume	To set the microphone volume.	Set the volume on the scale provided.
Set Speaker Volume	To set the speaker volume.	Set the volume on the scale provided.

Power

Table 3-14. Power Details

Power Setting Name	Description	Expected Value
Power Settings		
Device Power Plan	The general power plan of the thin client device.	Select from Balanced or Power Saver .
Power Settings on Battery		
Device Sleep Plan System Standby for WES2009 systems.	The time limit after which the device goes in to sleep mode.	Select an option from the drop-down list.
Dim Display Turn off Hard Drives for WES2009 systems.	The time limit after which the display is dimmed in order to save the battery.	Select an option from the drop-down list.
Turn off Display	The time limit after which the display is turned off in order to save the battery.	Select an option from the drop-down list.
Power Settings when Plugged in		
Device Sleep Plan System Standby for WES2009 systems.	The time limit after which the device goes in to sleep mode.	Select an option from the drop-down list.
Dim Display Turn off Hard Drives for WES2009 systems.	The time limit after which the display is dimmed when the thin client device is plugged in to the power outlet.	Select an option from the drop-down list.
Turn off Display	The time limit after which the display is turned off when the thin client device is plugged in to the power outlet.	Select an option from the drop-down list.

OS Configuration

The OS Configuration area enables you to set the configurations for various settings on the operating system that includes:

- **Browser, Firewall, and Aero**: to configure browser, firewall, and aero related settings.
- **Clocks**: to configure the clock settings. This is not applicable to WES2009 systems.
- **Other Settings** : to configure the **Appliance Mode** settings.

Browser, Firewall, and Aero

Table 3-15. Browser, Firewall, and Aero Details

Setting Name	Description	Expected Value
Internet Explorer Proxy Settings		
Proxy	The proxy bypass server.	True or False. If set to True, you need to provide the details of the Proxy Bypass Server.
Host Name or IP Address	The host name or IP address of the proxy bypass server.	Enter the IP address if you have set the Proxy to True .
Proxy Auto Config	The proxy auto configuration file to configure Internet Explorer.	Enter the file name.
Proxy Auto Detect	To automatically detect the proxy bypass server.	True or False. Automatically sets to True if Proxy is set to True and to False if Proxy is set to False .
Proxy Server Port	The proxy bypass server port.	Defaults to 80. Leave the default value or change the port number as configured.
Internet Explorer Settings		

Table 3-15. Browser, Firewall, and Aero Details

Setting Name	Description	Expected Value
AutoStart	To automatically start Internet Explorer in full-screen mode.	True or False. NOTE: If you set this to True , then you cannot set the Appliance Mode for Internet Explorer.
Home Page	The home page for the Internet Explorer.	Enter the URL or the address of the home page. For example, www.dellwyse.com .
IE Favourites and Trusted Sites	The list of all the favourite and trusted Sites.	Click the button to launch the IE Favourites and Trusted Sites window. Click Add Row to add a record to the grid. Enter the details of the favourites, trusted sites, and shortcuts. Click Apply and Exit . NOTE: If you check Shortcut for a particular URL, a shortcut is created on the thin client desktop.
Internet Zone Security Level	The security setting for Internet Explorer in internet zone.	Select an option from the drop-down list.
Local Zone Security Level	The security setting for Internet Explorer in the local or intranet zone.	Select an option from the drop-down list.
Restricted Zone Security Level	The security setting for Internet Explorer in restricted sites.	Select an option from the drop-down list.
Trusted Zone Security Level	The security setting for Internet Explorer in trusted sites.	Select and option from the drop-down list.

Clocks

Table 3-16. Clock Details

Clock Setting Name	Description	Expected Value
Clock1 Settings		
Clock	To enable or disable the clock.	True or False.
Display Name	The display name for the clock.	Enter a display name.
Timezone Name	The name of the timezone to which the clock is to be set.	Select an option from the drop-down list.
Clock2 Settings		
NOTE: This option is not available for WES2009.		
Clock	To enable or disable the second clock.	True or False.
Display Name	The display name for the second clock.	Enter a display name.
Timezone Name	The name of the timezone to which the second clock is to be set.	Select an option from the drop-down list.

Other Settings

You can enter the Appliance Mode settings in this area. Appliance mode allows a supported thin client to be used as a dedicated device for a specific application. You can log in to the device to be immediately presented with your remote client log in, a local full-screen, Internet Explorer, or are logged into a remote session. Appliance mode can be especially beneficial for kiosks, digital displays, advertising displays, and dedicated usage.



NOTE: Appliance mode requires that WCM settings are not applied in Append mode. To disable Append mode, open the Options menu and clear/uncheck Append Settings.

Table 3-17. Other Setting Details

Setting Name	Description	Expected Value
Appliance Mode Settings		
Appliance Mode	To turn the thin client device into a dedicated device for a remote connection.	Off or any of the values from the drop-down list. NOTE: If you have set the VMware View, Ctrix, vWorkspace, RDP, or Internet Explorer Autostart feature to True , then you must set it to False before selecting any option from the drop-down list.
Exit from Appliance Mode	To shut down from appliance mode.	True or False.
Exit Key (+ CTRL + Shift)	The key used along with control and shift keys to exit from the appliance mode.	Enter a key value from A-Z or 0-9.
Log Out Appliance Mode	To log out from the appliance mode.	True or False.
Restart Appliance Mode	To restart appliance mode.	True or False.
Shut Down Appliance Mode	To shut down the appliance mode.	True or False.
Generic Appliance Mode : You can configure the appliance mode for any specific application of your choice.		

Table 3-17. Other Setting Details *(continued)*

Setting Name	Description	Expected Value
Appliance Command Line	The command line parameter to be run to launch the application in appliance mode.	Enter the command line parameter to run the application of your choice. For example, if you want to run Notepad or Calculator in the appliance mode, enter Notepad.exe or Calc.exe . If you want to run a specific application enter the complete path from where the application executable is to be launched.
Appliance Mode Name	The name for the appliance mode application.	Enter a name for the application.
Configuration Description		
Description	General description for the configuration file.	Enter a general description for the configuration file.

Appliance Mode is supported for:

- VMware View connections
- Citrix XenApp, XenDesktop, and Secure Gateway connections
- One or more RDP/RDS/Terminal Server connections
- Internet Explorer
- Quest vWorkspace
- Any locally installed application on the thin client. (Generic Appliance Mode).



NOTE: Appliance Mode for Internet Explorer does not support Citrix sessions launched from Internet Explorer.

An **Exit** button is now available for all Appliance Mode applications. This allows you to exit, log out, shut down, or restart from the client while in Appliance Mode.

The **Exit** button is supported for Citrix XenDesktop, and VMware Horizon View Appliance Mode applications with some limitations. You can also configure the exit buttons and shortcuts as per user requirements.

Appliance Mode Workflow on Thin Client Devices

- 1 Boot the operating system on the thin client system.
- 2 Log in to the system.
- 3 The WCM automatically downloads the WCM XML configuration file from the FTP or IIS Web Server or uses a locally stored file on the thin client.
- 4 WCM applies the XML file settings including the Appliance mode.
- 5 Use the thin client system with the configured Appliance mode session.
- 6 Log off from the system or session.

After you log out from the system or session, you can again log in to the system at a later point. In Appliance mode, you only need to press the **Ctrl-Alt-Del** keys to shut down the current session or restart the system again.

Disabling or Stopping the Appliance Mode

You need to log in as Administrator to disable or log out of the Appliance mode by using one of the following options:

- **Server deployed WCM XML files** — Change the WCM XML file from **WCM Application** → **OS Configuration** → **Other Settings** on the deployment server.
- **By using the thin client** — On the thin client:
 - a Hold down the **Shift** key while logging off the server.
 - b Log in as an Administrator and while the WCM Appliance mode is downloading or applying the XML file, select the WCM splash screen with your mouse and press the **Esc** key.

This disables Appliance mode in that session. You can then disable the **Write-Filter** and make the necessary changes.

Agent Settings

You can use this option in the **Options** menu to configure your default client agent settings. These settings are required if you are using Dell Wyse Device Manager (WDM) to push the configuration files to your thin clients.



NOTE: You must configure the WDM Server if you want to use it to push the configuration files to the thin clients. For more information, see [Configuring the Dell Wyse Device Manager \(WDM\) Server](#).

To configure Agent Settings:

- 1 Log in to the Repository Server as Administrator and launch the WCM Application GUI.
- 2 Select **Options** → **Agent Settings** on the menu.
- 3 In the **Agent Settings** dialog box, enter the following:
 - **Protocol** — Select an option from the drop-down box.
 - **Server IP** — Enter the IP address of the Repository Server.
 - **Port** — This is entered by default based on the protocol you choose.
 - **Path** — Enter the path of the configuration file. This is optional.
 - **User Name** — Enter the server username. This is optional.
 - **Password** — Enter the server password. This is optional.
- 4 Select one or more of the following options:
 - **Import Configuration on Every Boot** — if you want to download the configuration file everytime the thin client system reboots.
 - **Use WDM** — if you want to use the WDM server to push the configuration file to the thin client.
 - **Enable Balloon Tips** — if you want a balloon tip to indicate the status of download on the thin clients.
- 5 Click **Apply** to save your settings.

Using Your Configuration Files

After you create the configuration file, you must store the file in the location you need, and then complete the procedures required to apply the configurations to the thin clients systems.

You can deploy WCM configuration files to your thin clients:

- Automatically — For more information, see [Setting Up Automatic Configuration](#).
- Manually — For more information, see [Setting Up Manual Configuration](#).



NOTE: Ensure that the File Based Write Filter of the thin client is enabled. The WCM Client will not download and apply settings if the File Based Write Filter is disabled.

Setting Up Automatic Configuration

For the thin client systems to access configuration files from a server and update themselves automatically:

- 1 Place your configuration files on the server. On your server, you must set up the correct folder. For more information on setting up the folder structure, see [step 8](#) under [Configuring the Repository Server](#).
- 2 Direct your thin client systems to the server using the DNS SRV, DNS Hostname, or DHCP Options. For more information, see [Discovery Settings for the WCM Server](#) and [Configuring the WCM Thin Client Systems](#).

Your thin client systems check at each boot up to see if updates are available on your predefined server.

- 3 Reboot or log out from your thin client systems.

A system reboot generates the **Discovery.ini** file, which redirects the system to download the configuration file from the repository server. If updates are available, the updates are automatically installed. For example, new connections available to a user on the configuration file.

Setting Up Manual Configuration

For the thin client systems to successfully access configuration files and update themselves manually using the **Import** feature of the WCM Client on the thin client:

- 1 Place your configuration files in a local or remote location that is accessible by the thin client.
- 2 Import the configuration file by using the Import feature on the WCM Client. For more information, see [Importing Thin Client Configurations](#).

Using the Dell Wyse Configuration Manager (WCM) Client

This chapter discusses how to use the WCM Client that is installed on the thin client systems. You can manually import configuration files, export configuration files, view configuration history, and configure the DHCP settings on the client system.

Launching the WCM Client

You need to log in to the thin client system as an Administrator to launch the WCM Client.

The WCM Client does not have any shortcuts on the thin client desktop.

To launch the WCM Client, navigate to the Control Panel from the **Start** menu and click the **WCM** icon.

The top panel of the application displays the details of the configuration file that is currently being applied to the thin client system.

Importing Thin Client Configurations

To manually import the configuration file:

- 1 Launch the WCM Client from the control panel.
- 2 Click **Import Configuration**. The fields are displayed on the right panel.
- 3 Select one of the following options:
 - **Local** — if you have saved the configuration files locally on the thin client system, a network drive, or on a USB drive and want to download the configuration files. Browse to the location, select the file, and click **Open**.
 - **Remote** — if you have saved the configuration files on the repository server in a remote location. Follow the steps given below:
 - Select the **Protocol** from the drop-down list.
 - Enter the **Server IP** address of the repository server.

- The Port is displayed by default. The default ports for FTP, HTTP, and HTTPS are 21, 80, and 443 respectively.
- Enter the folder **Path** where the configuration file is saved in the remote location if you have not used the default path.
- Enter the **Username** and **Password** to access the Repository server.



NOTE: If you have been deploying your configuration files locally and the Protocol is set to **Local** in the **Agent Settings** dialog box of the WCM Application GUI and Import Configuration is set to **Local** in the **Import Configuration** dialog box of the WCM Client, you can switch back to a remote download of the configuration files. You must set the **Protocol** to **FTP**, **HTTP**, or **HTTPS** using the **Agent Settings** dialog box of the WCM Application GUI. You must also ensure that you set the Import Configuration to **Remote** in the **Import Configuration** dialog box of the WCM Client. You cannot switch back to a remote download using only the **Agent Settings** dialog box of the WCM Application GUI.

- 4 If you want the configuration file to be imported everytime the thin client system boots, check the **Import configuration on every boot** option.



NOTE: If the **Import configuration on every boot** option is selected, the WCM remote repository is discovered in the following order of preference **DNS-SRV**, **DNS-Host**, **DHCP Options**, **Registry Settings** in the remote settings. If none of the above are configured, then the **Import configuration on every boot** option is not implemented.

- 5 Click **Save Settings**.
- 6 Click **Import** to apply the settings in the configuration file to the thin client system immediately.

Fallback Mechanism for Failed Download of Configuration File

If you have configured the DNS-SRV, DNS-Host, DHCP Options, and Registry Settings in the remote settings, and the configuration file does not download, then the fallback mechanism for each of the preceding mechanisms is as follows:

- 1 For a device specific configuration or for a local user, if the **WE8SConfig.xml**, or **WES7Config.xml**, or **WESConfig.xml** fails to download from the remote path, check the configuration history for the same named latest configuration and apply that file.

- 2 For a domain-joined user, if the **administrator.xml** fails to download from the remote path, download the **WE8SConfig.xml**, or **WES7Config.xml**, or **WESConfig.xml** from the same remote path and apply that file.
If that too fails to download, check the configuration history for the **WE8SConfig.xml**, or **WES7Config.xml**, or **WESConfig.xml** latest configuration and apply that file.
- 3 If the **xml** fallback for each discovery method also fails, then the Factory Default file is applied.

Exporting Thin Client Configurations

To export the configurations on a thin client system to a configuration file:

- 1 Launch the WCM Client from the control panel.
- 2 Click **Export Configuration**.
- 3 Enter the file name with a **.xml** extension. For example, **TestWES.xml** (for WES2009) or **TestWES7.xml** (for WES7) or **TestWES8.xml** (for WE8S).
- 4 Use the **Browse** command button to select the local location where you want to save the file (such as a USB drive).
- 5 Click **Export** to export and save the current configurations of the thin client to the configuration file.

Using Configuration History

You can use the **Configuration History** option to apply a configuration file that was previously used on the thin client. This option is useful when a new file did not get applied successfully.

To apply the configuration file:

- 1 Launch the WCM Client from the control panel.
- 2 Click **Configuration History**.
The five most recent and successfully imported configuration files are displayed.
- 3 Select the configuration file you want to import from the list.

- 4 Click **Import** to apply the file to the thin client system immediately.
- 5 Click **Delete** to delete a configuration file from the list. If you have downloaded the file from a remote server, then it does not delete the file from the server.



NOTE: You cannot delete the factory default configuration file.

Manually Setting Debug Options on a Thin Client

The WCM Debugging dialog box allows you to manually set debug options on the thin client. Setting the debug options enables you to troubleshoot issues with the thin client by reviewing the debug log file that is created if this option is configured.

To set the debug options:

- 1 Launch the WCM Client from the control panel.
- 2 Click **Debug Settings** to launch the **WCM Debugging** window.
- 3 Select the **Debug Mode** from one of the following options:
 - **File Logging** — This is the default option and stores debug messages in the **wcmdebug** file in **C:\Users\Public\Documents** on **WE8S** and **WES7** thin clients, or in **C:\Documents and Settings\All Users\Documents\Wyse** on **WES2009** thin clients.
 - **Verbose** — This option sends debug messages to the Microsoft **DbgView** utility running locally on the thin client.
- 4 Select the **Debug Level** from one of the following options:
 - **Level 1 (Informational)** — Includes informational messages only.
 - **Level 2 (Errors)** — Includes informational messages and error messages only.
 - **Level 3 (Debug)** — Includes informational messages, error messages, and debugging messages.
- 5 Click **OK** to apply the debug settings.

Typical Use Case Scenarios

This section describes the typical use case scenarios that can be performed using the Wyse Configuration Manager (WCM).

Case 1 - Using a Single Configuration for Multiple Thin Client Users

If you have multiple thin client systems with the same operating system installed on them (WE8S, WES7, or WES2009), you can use a single configuration to configure all the systems.

To perform this activity:

- 1 Log in as Administrator into any one of the thin client systems.
- 2 Ensure that the thin client system has the latest version of WCM Client installed on it.
- 3 Configure the thin client using the operating system functions.
- 4 Launch the WCM Client from the control panel.
- 5 Click **Export Configuration** to export the configuration file to a remote location on the repository server. For more information, see [Exporting Thin Client Configurations](#).
- 6 Ensure that the other thin client systems are able to connect to the repository server.

For more information on configuring the repository and the DNS/DHCP servers, see [Configuring the Repository Server](#) and [Discovery Settings for the WCM Server](#).

The thin client systems can connect to the Repository Server, download the exported configuration file, and apply the configurations automatically.

Case 2 - Using Multiple Configuration Files for Multiple Thin Client Users

If you have multiple thin client systems with the same operating system installed on them (WE8S, WES7, or WES2009), you can create multiple user specific configuration files and configure other thin clients running the same operating system.

To perform this activity:

- 1 Log in as Administrator into the thin client systems.
- 2 Ensure that the thin client systems have the latest version of WCM Client installed on them.
- 3 Configure multiple thin client systems using the Operating System functions.
- 4 Use the **Export Configuration** option on the WCM Client to export the configuration files to a remote location on the Repository Server. For more information, see [Exporting Thin Client Configurations](#).
- 5 Ensure that you place the configuration files in user specific folders on the Repository Server.

The other thin clients running WE8S, WES7, WES2009 run the WCM Client to retrieve and apply user specific configuration files through the network using their specified user log-in credentials.

Case 3 - Editing Specific Configuration Files for Thin Client Users

If you have created user specific configuration files for thin client users, then you can edit specific files and update the configurations as per the request of the users and enable them to update their systems.

To perform this activity:

- 1 Log in as Administrator into the specific thin client system where you have created a user specific configuration file.
- 2 Change the configuration of the system using the Operating System functions.

- 3 Use the **Export Configuration** option on the WCM Client to export the changed configuration file to the user specific folder on the Repository Server.
- 4 You can then log out and log in to the thin client system where you want the changes, and retrieve the configuration file from the Repository Server through the DNS/DHCP connection. For more information on configuring the Repository and the DNS/DHCP servers, see [Configuring the Repository Server](#) and [Discovery Settings for the WCM Server](#).

Case 4 - Selecting Specific Configuration Files Using a Thin Client on the Network

If you want to revert to any of the previous configurations for the thin client system, perform the following steps:

- 1 Log in as Administrator into the thin client system.
- 2 Launch the WCM Client on the system.
- 3 Click **Configuration History**. The five most recent and successfully imported configuration files are displayed.
- 4 Select configuration file you want to import from the list.
- 5 Click **Import** to apply the file to the thin client system immediately.
- 6 You can check the **Import configuration on every boot** option in the **Import Configuration** screen to import the configuration everytime you log in to the system.

Case 5 - Applying Specific Configuration Files to a Mobile Thin Client

If you receive a user request to access a user specific configuration file from a home network, perform the following steps:

- 1 Log in to the Repository Server as an administrator.
- 2 Navigate to the user specific folder location to access the configuration file.
- 3 Place the file on a HTTP server in a demilitarized zone (DMZ).

A DMZ is a computer host or a small network inserted as a neutral zone between a private network within the company and the public network outside the company.

- 4 Instruct the user to log in and connect to the HTTP server through the home network.
- 5 When the user logs in, the configuration settings are applied to the mobile thin client from the HTTP server over the home network.

Case 6 - Applying Configuration Files for New or Different Thin Client Users

If you want to re-configure a thin client for a new or a different user, perform the following steps:

- 1 Log in to the Repository Server as administrator and launch the WCM GUI.
- 2 Edit the configuration settings in an existing file. For more information, see [Editing Existing Configuration Files](#).
- 3 Copy the configuration file to a USB key.
- 4 Log in as administrator into the thin client system that you want to re-configure.
- 5 Launch the WCM Client on the thin client system and click the **Import Configuration** option.
- 6 Insert the USB key to the thin client, select **Local**, and enter the USB path of the configuration file.
- 7 Click **Import** to remove all the previous configurations and apply the desired configurations from the local USB key.

Appendix

Troubleshooting Devices That Cannot Locate Configuration Files

To successfully troubleshoot devices that cannot locate their configuration files, it is important to understand the DNS-based discovery process used by the WCM agent on the device.

If you use the repository server to deploy your configuration files and your thin clients access the configuration files automatically through FTP, HTTP, or HTTPS, the process by which the configuration files are obtained by the WCM agent on the thin client is in the following order:

- 1 **DNS Service Lookup** — Note that this is only if the remote deployment option is implemented. For more information, see [DNS Service Record Lookup](#).
- 2 **DNS Hostname Lookup** — Note that this is only if the remote deployment option is implemented. For more information, see For more information, see [DNS Service Record Lookup](#).
- 3 **DHCP Options** — For more information, see [DHCP Option Tags Lookup](#).
- 4 Configured location where you placed the configuration file, which could be either of the following:
 - **Local Location** — such as a C: drive, local network folder, or USB drive that you set in the **Local** option of the **Import Configuration** screen in the WCM Client.
For more information, see [Importing Thin Client Configurations](#).
 - **Remote Location** — such as a remote server location that you set in the **Remote** option of the **Import Configuration** screen in the WCM Client.
For more information, see [Importing Thin Client Configurations](#).

- 5 **Local Factory Default Files** — If the values necessary to find the configuration file are not successfully obtained from DNS, the WCM agent tries the DHCP Options, and so on.

If there is no location set in the **Import Configuration** screen on the thin client, or if the thin client cannot reach these locations, the thin client uses the factory default **WESConfig.xml**, or **WES7Config.xml**, or the **WESConfig.xml** file on the thin client. This is the latest configuration file updated to the folder on the thin client.

The local default configuration file location for the WES2009 (WESConfig.xml), WES7 (WES7Config.xml), WE8S (WE8SConfig) files is **C:\Program Files\Wyse\WCM\Agent**.